APRIL/MAY 2024

CECA63B/CECS63B — CRYPTOGRAPHY

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define the term computer security.
2. What is called security attack?
3. List out some AES transformations.
4. What is block cipher principle?
5. What is elliptic curve cryptography?
6. State the meaning of pseudo random number.
7. Define the term CMAC.
8. What is the importance of HMAC?
9. Define the term Email.
10. What is called web security?

PART B — (5 × 5 = 25 marks)

Answer ALL the questions.

11. (a) Explain about the challenges of computer security.

Or

(b) Discuss on security attack surfaces.

12. (a) Elaborate on any two substitution techniques.

Or

(b) Describe briefly on transposition techniques.

13. (a) Write about public key cryptography.

Or

(b) Explain about elliptic curve over zp.

14. (a) Discuss on secure hash algorithm.

Or

(b) Elaborate on the concept of MAC security.

15. (a) Describe firewall generations in detail.

Or

(b) Write notes on various email formats.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain the different security attacks.

17. Discuss on symmetric cyber model in detail.

18. Describe in detail about RSA algorithm.

19. Write about the applications of cryptography hash functions.

20. Describe the web security considerations in detail.

———————